Protect Yourself from Identity Theft

Identity theft is on the rise as Internet usage increases on a daily basis and more information and purchases are made available over the Internet.

If a thief obtains personally identifiable information (PII) through a social networking site, such as Facebook or MySpace, it can be added to already known information and your identity and credit are at risk.

With Internet social networking in people's daily lives to include allowing social networking within our work environment, people open themselves, family members, and jobs to risks and threats, which have to be monitored closely by all. Network security devices cannot protect people against themselves.

Computer incidents are on the rise within work environments. For Airmen, Soldiers and their families affected this can have a devastating effect on their personnel lives and well-being. E-mail scams, phishing attempts, computer viruses, identity theft, and loss of PII have become a daily fact of life.

Now social networking sites are being used as a delivery tool for these threats. Always remember operational security when using and visiting social network sites. It's the user who is responsible for all actions and no security device can stop those interactions.

Some purchases can be made over the Internet without ever physically having a credit or debit card. All a thief needs is a person's name, a card number, an expiration date, the three-digit security code on the back and the billing address, usually a person's home address.

A quick search of a person's name on a social networking site can reveal a home address if it is posted openly or a person doesn't have security settings configured correctly. A thief can also check phonebook records to determine addresses as well.

The latest scam typically involves servicemembers who don't have Facebook accounts, suddenly discovering that someone has created accounts in their name for the purposes of defrauding others for financial gain. The scam artist typically befriends individuals online in chat rooms or via e-mail, while posing as a National Guard member. They attempt to ensnare long-time acquaintances of the servicemember, who unwittingly "friend" the scam artist posing as the Soldier or Airman.

The fake Facebook pages typically have enough correct personal information obtained online, includes photos, to convince strangers and acquaintances they are viewing the servicemember's real Facebook site.

The con artist may also claim to be deploying or redeploying and be in need of financial assistance, seeking romantic engagements, or suffered the recent loss of a loved one to play on the sympathy of others. The potential scenarios are unfortunately far too numerous to list, but no less disturbing.

Typically a servicemember will not become aware of the con until an acquaintance or a suspicious victim contacts the member's unit, family, or other sources to confirm elements of the scam. Therefore, if it comes to your attention that you may be the victim of this type of Internet fraud, you may contact Facebook and report the abuse here, http://www.facebook.com/help/?topic=security.

You should report identity theft to the Internet Crime Complaint Center (IC3) at http://www.ic3.gov/default.aspx. The IC3 is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance, and accepts online Internet crime complaints from either the person who believes they were defrauded or from a third party to the complainant.

It may also be in your best interests to contact your credit card company, or companies, to submit a fraud alert. You should also contact the three credit bureaus, who by law are required to provide you with one free credit report each per year. These credit bureaus also have separate fraud alert services available for active-duty military personnel.

Another good source of information for those who wish to educate themselves about online scams is the US Federal Trade Commission internet fraud website: http://www.econsumer.gov/english

Each servicemember must be vigilant of the risks of using social networking sites, as well as the multitude of other threats to their personal and financial well-being and the unwitting voluntary disclosure of PII.

-30-